Amendments to the Claims

Kindly amend claims 1, 3, 9-11, 16-21, 23, 25, 26, 27, 29, 35-37, 42-47, 49, 51-54, 56, 62-64, 69-74, 76, 78 & 79, and cancel claims 2, 7, 8, 12, 14, 15, 22, 28, 33, 34, 38, 40, 41, 48, 55, 60, 61, 65, 67, 68 & 75 (without prejudice), as set forth below. All pending claims are reproduced below, with changes in the amended claims shown by underlining (for added matter) and strikethrough/double brackets (for deleted matter).

1. (Currently Amended) An authenticated identity translation method comprising:

establishing an authenticated user identity at an initial server responsive to an identification and authentication event within a domain comprising [[an]] said initial ~~authentication unit~~ server and [[a]] at least one subsequent ~~authentication unit~~ server, said identification and authentication event occurring at said initial ~~authentication unit~~ server, said initial ~~authentication unit~~ server and said at least one subsequent ~~authentication unit~~ server employing disparate user registries with different user identities, said disparate user registries being separately maintained by the servers and being logically represented in a global registry maintained by a domain controller, said global registry including information that establishes a correspondence between a user identity in the initial server with a corresponding, local user identity within the at least one subsequent server;

generating a translation token representative of said identification and authentication event ~~to be forwarded to said subsequent authentication unit;~~ and providing said translation token to said domain controller, storing said translation token by said domain controller and obtaining a token reference from said domain controller, said token reference comprising an index to said stored translation token within said domain controller;

forwarding said token reference from the initial server to said at least one subsequent server along with a request; and

translating the authenticated user identity of said initial ~~authentication unit~~ server to a local user identity of said at least one subsequent ~~authentication unit~~ server, wherein said at least one subsequent ~~authentication unit~~ server initiates said translating employing said token reference received from said initial server, said translating comprising:

forwarding said token reference from the at least one subsequent server to said domain controller, and employing said token reference at the domain controller to retrieve said translation token and translate the authenticated user identify of said initial server to the local user identity of said at least one subsequent server employing said global registry of said corresponding user identities maintained by the domain controller.

2. (Canceled).

3. (Currently Amended) The method of claim [[2]] 1, wherein ~~the token comprises a translation token,~~ said translation token ~~including~~ includes at least some of an identity of the initial ~~authentication unit~~ server, a user identity, ~~a method of authentication employed,~~ and a time stamp representative of time of authentication.

4. (Original) The method of claim 3, wherein said generating further comprises obtaining signing value pair information from the domain controller, and signing the translation token using said signing value pair.

5. (Original) The method of claim 4, wherein said translating by the domain controller further comprises validating the translation token signature prior to said translating of the authenticated user identity to the local user identity using the global registry of different user identities.

6. (Original) The method of claim 5, wherein said signing value pair comprises a signing value and a sequence number, and wherein said sequence number is encrypted by the domain controller employing an encryption key known only to the domain controller, and said validating includes employing the encryption key to validate the translation token.

7. (Canceled).

8. (Canceled).

9. (Currently Amended) The method of claim [[2]] 1, further comprising authenticating the local user identity at the at least one subsequent ~~authentication unit~~ server, said authenticating being based on a return code received from the domain controller with the local user identity, said return code being based on at least one authentication policy for the domain.

10. (Currently Amended) The method of claim 9, wherein said at least one authentication policy is at least one of user dependent or method of authentication dependent for said at least one subsequent ~~authentication unit~~ server, and wherein the method of authentication comprises a method of authentication employed by said establishing of said authenticated user identity at said initial ~~authentication unit~~ server.

11. (Currently Amended) The method of claim [[2]] 1, further comprising repeating said method for at least one additional subsequent ~~authentication unit~~ server, wherein with each repeating, said at least one subsequent ~~authentication unit~~ server becomes said initial ~~authentication unit~~ server and said at least one additional subsequent ~~authentication unit~~ server becomes said at least one subsequent ~~authentication unit~~ server, wherein said domain controller is employed by each at least one additional subsequent ~~authentication unit~~ server in translating the token to a respective local user identity.

12. (Canceled).

13. (Original) The method of claim 1, wherein the domain comprises a trust domain, and wherein the method further comprises initially establishing said trust domain within which the authenticated identity translation is to occur.

14. (Canceled).

15. (Canceled).

16. (Currently Amended) The method of claim 1, wherein said method further comprises one of forwarding the token to the at least one subsequent ~~authentication unit~~ server directly from the initial ~~authentication unit~~ server or forwarding the token from the initial ~~authentication unit~~ server through a user of the initial ~~authentication unit~~ server to the at least one subsequent ~~authentication unit~~ server.

17. (Currently Amended) The method of claim 1, wherein the initial ~~authentication unit~~ server and the at least one subsequent ~~authentication unit~~ server reside in different partitions of a multi-partition computing environment.

18. (Currently Amended) The method of claim 1, wherein the initial ~~authentication unit~~ server is also another subsequent ~~authentication unit~~ server to a further initial ~~authentication unit~~ server establishing another authenticated user identity.

19. (Currently Amended) The method of claim 18, wherein the at least one subsequent ~~authentication unit~~ server comprises said further initial ~~authentication unit~~ server.

20. (Currently Amended) The method of claim 1, further comprising repeating said method for multiple users, employing multiple initial ~~authentication unit~~ servers, each requiring access to at least one subsequent ~~authentication unit~~ server.

21. (Currently Amended) The method of claim 1, wherein said domain comprises a heterogeneous computing network, and wherein said initial ~~authentication unit~~ server and said at least one subsequent ~~authentication unit~~ server comprise heterogeneous computing units.

22. (Canceled).

23. (Currently Amended) The method of claim 1, wherein the generating further comprises securing the token reference against modification prior to said forwarding of the token reference to said at least one subsequent ~~authentication unit~~ server.

24. (Original) The method of claim 1, wherein a structure of said token is programmable by an administrator of said domain.

25. (Currently Amended) The method of claim 1, ~~wherein the domain further comprises a domain controller, and~~ wherein said method further comprises performing by the domain controller at least one of retiring the token or purging the token subsequent to said translating.

26. (Currently Amended) The method of claim 1, wherein said method further comprises employing a secure protocol to transfer [[a]] said request and said token reference from said initial ~~authentication unit~~ server to said at least one subsequent ~~authentication unit~~ server.

27. (Currently Amended) An authenticated identity translation system comprising:

means for establishing an authenticated user identity at an initial server responsive to an identification and authentication event within a domain comprising [[an]] said initial ~~authentication unit~~ server and [[a]] at least one subsequent ~~authentication unit~~ server, said identification and authentication event occurring at said initial ~~authentication unit~~ server, said initial ~~authentication unit~~ server and said at least one subsequent ~~authentication unit~~ server employing disparate user registries with different user identities, said disparate user registries being separately maintained by the servers and being logically represented in a global registry maintained by a domain controller, said global registry including information that establishes a correspondence between a user identity in the initial server with a corresponding, local user identity within the at least one subsequent server;

means for generating a translation token representative of said identification and authentication event ~~to be forwarded to said subsequent authentication unit;~~ and providing said translation token to said domain controller, storing said translation token by said domain controller and obtaining a token reference from said domain controller, said token reference comprising an index to said stored translation token within said domain controller;

means for forwarding said token reference from the initial server to said at least one subsequent server along with a request; and

means for translating the authenticated user identity of said initial ~~authentication unit~~ server to a local user identity of said at least one subsequent ~~authentication unit~~ server, wherein said at least one subsequent ~~authentication unit~~ server initiates said translating employing said token reference received from said initial server, said translating comprising:

forwarding said token reference from the at least one subsequent server to said domain controller, and employing said token reference at the domain controller to retrieve said translation token and translate the authenticated user identify of said initial server to the local user identity of said at least one subsequent server employing said global registry of said corresponding user identities maintained by the domain controller.

28. (Canceled).

29. (Currently Amended) The system of claim [[28]] 27, wherein ~~the token comprises a translation token,~~ said translation token ~~including~~ includes at least some of an identity of the initial ~~authentication unit~~ server, a user identity, ~~a method of authentication employed,~~ and a time stamp representative of time of authentication.

30. (Original) The system of claim 29, wherein said means for generating further comprises means for obtaining signing value pair information from the domain controller, and for signing the translation token using said signing value pair.

31. (Original) The system of claim 30, wherein said means for translating by the domain controller further comprises means for validating the translation token signature prior to translating of the authenticated user identity to the local user identity using the global registry of different user identities.

32. (Original) The system of claim 31, wherein said signing value pair comprises a signing value and a sequence number, and wherein said sequence number is encrypted by the domain controller employing an encryption key known only to the domain controller, and said means for validating includes means for employing the encryption key to validate the translation token.

33. (Canceled).

34. (Canceled).

35. (Currently Amended) The system of claim [[28]] 27, further comprising means for authenticating the local user identity at the at least one subsequent ~~authentication unit~~ server, said authenticating being based on a return code received from the domain controller with the local user identity, said return code being based on at least one authentication policy for the domain.

36. (Currently Amended) The system of claim 35, wherein said at least one authentication policy is at least one of user dependent or method of authentication dependent for said at least one subsequent ~~authentication unit~~ server, and wherein the method of authentication comprises a method of authentication employed by said means for establishing of said authenticated user identity at said initial ~~authentication unit~~ server.

37. (Currently Amended) The system of claim [[28]] 27, further comprising means for repeating said system for at least one additional subsequent ~~authentication unit~~ server, wherein with each repeating, said at least one subsequent ~~authentication unit~~ server becomes said initial ~~authentication unit~~ server and said at least one additional subsequent ~~authentication unit~~ server becomes said at least one subsequent ~~authentication unit~~ server, wherein said domain controller is employed by each at least one additional subsequent ~~authentication unit~~ server in translating the token to a respective local user identity.

38. (Canceled).

39. (Original) The system of claim 27, wherein the domain comprises a trust domain, and wherein the system further comprises means for initially establishing said trust domain within which the authenticated identity translation is to occur.

40. (Canceled).

41. (Canceled).

42. (Currently Amended) The system of claim 27, wherein said system further comprises one of means for forwarding the token to the at least one subsequent ~~authentication unit~~ server directly from the initial ~~authentication unit~~ server or means for forwarding the token from the initial ~~authentication unit~~ server through a user of the initial ~~authentication unit~~ server to the at least one subsequent ~~authentication unit~~ server.

43. (Currently Amended) The system of claim 27, wherein the initial ~~authentication unit~~ server and the at least one subsequent ~~authentication unit~~ server reside in different partitions of a multi-partition computing environment.

44. (Currently Amended) The system of claim 27, wherein the initial ~~authentication unit~~ server is also another subsequent ~~authentication unit~~ server to a further initial ~~authentication unit~~ server establishing another authenticated user identity.

45. (Currently Amended) The system of claim 44, wherein the at least one subsequent ~~authentication unit~~ server comprises said further initial ~~authentication unit~~ server.

46. (Currently Amended) The system of claim 27, further comprising means for repeating said system for multiple users, employing multiple initial ~~authentication unit~~ servers, each requiring access to at least one subsequent ~~authentication unit~~ server.

47. (Currently Amended) The system of claim 27, wherein said domain comprises a heterogeneous computing network, and wherein said initial ~~authentication unit~~ server and said at least one subsequent ~~authentication unit~~ server comprise heterogeneous computing units.

48. (Canceled).

49. (Currently Amended) The system of claim 27, wherein the means for generating further comprises means for securing the token reference against modification prior to said forwarding of the token reference to said at least one subsequent ~~authentication unit~~ server.

50. (Original) The system of claim 27, wherein a structure of said token is programmable by an administrator of said domain.

51. (Currently Amended) The system of claim 27, ~~wherein the domain further comprises a domain controller, and~~ wherein said system further comprises means for performing by the domain controller at least one of retiring the token or purging the token subsequent to said translating.

52. (Currently Amended) The system of claim 27, wherein said system further comprises means for employing a secure protocol to transfer [[a]] said request and said token reference from said initial ~~authentication unit~~ server to at least one said subsequent ~~authentication unit~~ server.

53. (Currently Amended) An authenticated identity translation system comprising:

a trusted domain comprising an initial ~~authentication unit~~ server, [[a]] at least one subsequent ~~authentication unit~~ server, and a domain controller, said initial ~~authentication unit~~ server and said at least one subsequent ~~authentication unit~~ server employing disparate user registries with different user identities, said disparate user registries being separately maintained by the servers and being logically represented in a global registry maintained by a domain controller, said global registry including information that establishes a correspondence between a user identity in the initial server with a corresponding, local user identity within the at least one subsequent server;

said initial ~~authentication unit~~ server being adapted to establish an authenticated user identity responsive to an identification and authentication event occurring thereat, and to generate a translation token representative of said identification and authentication event ~~to be forwarded to said subsequent authentication unit;~~ and providing said translation token to said domain controller, storing said translation token by said domain controller and obtaining a token reference from said domain controller, said token reference comprising an index to said stored translation token within said domain controller;

said initial server being adapted to forward said token reference from the initial server to said at least one subsequent server along with a request; and

said at least one subsequent ~~authentication unit~~ server being adapted to forward said translation token to the domain controller for translating the authenticated user identity of said initial ~~authentication unit~~ server to a local corresponding user identity of said at least one subsequent ~~authentication unit~~ server, wherein said translating includes employing said translation token received from said initial ~~authentication unit~~ server.

54. (Currently Amended) At least one program storage device readable by a machine, tangibly embodying at least one program of instructions executable by the machine to perform an authenticated identity translation method, said method comprising:

establishing an authenticated user identity at an initial server responsive to an identification and authentication event within a domain comprising [[an]] said initial ~~authentication unit~~ server and [[a]] at least one subsequent ~~authentication unit~~ server, said identification and authentication event occurring at said initial ~~authentication unit~~ server, said initial ~~authentication unit~~ server and said at least one subsequent ~~authentication unit~~ server employing disparate user registries with different user identities, said disparate user registries being separately maintained by the servers and being logically represented in a global registry maintained by a domain controller, said global registry including information that establishes a correspondence between a user identity in the initial server with a corresponding, local user identity within the at least one subsequent server;

generating a translation token representative of said identification and authentication event ~~to be forwarded to said subsequent authentication unit;~~ and providing said translation token to said domain controller, storing said translation token by said domain controller and obtaining a token reference from said domain controller, said token reference comprising an index to said stored translation token within said domain controller;

forwarding said token reference from the initial server to said at least one subsequent server along with a request; and

translating the authenticated user identity of said initial ~~authentication unit~~ server to a local user identity of said at least one subsequent ~~authentication unit~~ server, wherein said at least one subsequent ~~authentication unit~~ server initiates said translating employing said token reference received from said initial server, said translating comprising:

forwarding said token reference from the at least one subsequent server to said domain controller, and employing said token reference at the domain controller to retrieve said translation token and translate the authenticated user identify of said initial server to the local user identity of said at least one subsequent server employing said global registry of said corresponding user identities maintained by the domain controller.

55. (Canceled).

56. (Currently Amended) The at least one program storage device of claim [[55]] 54, wherein ~~the token comprises a translation token,~~ said translation token ~~including~~ includes at least some of an identity of the initial ~~authentication unit~~ server, a user identity, ~~a method of authentication employed,~~ and a time stamp representative of time of authentication.

57. (Original) The at least one program storage device of claim 56, wherein said generating further comprises obtaining signing value pair information from the domain controller, and signing the translation token using said signing value pair.

58. (Original) The at least one program storage device of claim 57, wherein said translating by the domain controller further comprises validating the translation token signature prior to said translating of the authenticated user identity to the local user identity using the global registry of different user identities.

59. (Original) The at least one program storage device of claim 58, wherein said signing value pair comprises a signing value and a sequence number, and wherein said sequence number is encrypted by the domain controller employing an encryption key known only to the domain controller, and said validating includes employing the encryption key to validate the translation token.

60. (Canceled).

61. (Canceled).

62. (Currently Amended) The at least one program storage device of claim [[55]] 54, further comprising authenticating the local user identity at the at least one subsequent ~~authentication unit~~ server, said authenticating being based on a return code received from the domain controller with the local user identity, said return code being based on at least one authentication policy for the domain.

63. (Currently Amended) The at least one program storage device of claim 62, wherein said at least one authentication policy is at least one of user dependent or method of authentication dependent for said at least one subsequent ~~authentication unit~~ server, and wherein the method of authentication comprises a method of authentication employed by said establishing of said authenticated user identity at said initial ~~authentication unit~~ server.

64. (Currently Amended) The at least one program storage device of claim [[55]] 54, further comprising repeating said method for at least one additional subsequent ~~authentication unit~~ server, wherein with each repeating, said at least one subsequent ~~authentication unit~~ server becomes said initial ~~authentication unit~~ server and said at least one additional subsequent ~~authentication unit~~ server becomes said at least one subsequent ~~authentication unit~~ server, wherein said domain controller is employed by each at least one additional subsequent ~~authentication unit~~ server in translating the token to a respective local user identity.

65. (Canceled).

66. (Original) The at least one program storage device of claim 54 , wherein the domain comprises a trust domain, and wherein the method further comprises initially establishing said trust domain within which the authenticated identity translation is to occur.

67. (Canceled).

68. (Canceled).

69. (Currently Amended) The at least one program storage device of claim 54, wherein said method further comprises one of forwarding the token to the at least one subsequent ~~authentication unit~~ server directly from the initial ~~authentication unit~~ server or forwarding the token from the initial ~~authentication unit~~ server through a user of the initial ~~authentication unit~~ server to the at least one subsequent ~~authentication unit~~ server.

70. (Currently Amended) The at least one program storage device of claim 54, wherein the initial ~~authentication unit~~ server and the at least one subsequent ~~authentication unit~~ server reside in different partitions of a multi-partition computing environment.

71. (Currently Amended) The at least one program storage device of claim 54, wherein the initial ~~authentication unit~~ server is also another subsequent ~~authentication unit~~ server to a further initial ~~authentication unit~~ server establishing another authenticated user identity.

72. (Currently Amended) The at least one program storage device of claim 71, wherein the at least one subsequent ~~authentication unit~~ server comprises said further initial ~~authentication unit~~ server.

73. (Currently Amended) The at least one program storage device of claim 54 , further comprising repeating said method for multiple users, employing multiple initial ~~authentication unit~~ servers, each requiring access to at least one subsequent ~~authentication unit~~ server.

74. (Currently Amended) The at least one program storage device of claim 54, wherein said domain comprises a heterogeneous computing network, and wherein said initial ~~authentication unit~~ server and said at least one subsequent ~~authentication unit~~ server comprise heterogeneous computing units.

75. (Canceled).

76. (Currently Amended) The at least one program storage device of claim 54, wherein the generating further comprises securing the token reference against modification prior to said forwarding of the token reference to said at least one subsequent ~~authentication unit~~ server.

77. (Original) The at least one program storage device of claim 54, wherein a structure of said token is programmable by an administrator of said domain.

78. (Currently Amended) The at least one program storage device of claim 54, ~~wherein the domain further comprises a domain controller, and~~ wherein said method further comprises performing by the domain controller at least one of retiring the token or purging the token subsequent to said translating.

79. (Currently Amended) The at least one program storage device of claim 54, wherein said method further comprises employing a secure protocol to transfer [[a]] said request and said token reference from said initial ~~authentication unit~~ server to said at least one subsequent ~~authentication unit~~ server.

* * * * *